Math 357
Expositional homework 01

Assigned: 2024–01–08 (M)
Due: 2024–01–22 (M)

The goal of this homework is to expand and explore our library of examples related to ring structure. In particular, we will explore concrete examples related to the following chain of (one-way) implications:

$$\text{field} \Rightarrow \text{ED} \Rightarrow \text{PID} \Rightarrow \text{UFD} \Rightarrow \text{ID} \tag{1}$$

where ED denotes euclidean domain, PID denotes principal ideal domain, UFD denotes unique factorization domain, and ID denotes integral domain.

Let $\mathbf{Z}$ denote the ring of integers.

(a) Define each of the algebraic structures in (1).

(b) Give an example of a ring that is not an integral domain. Justify your assertion.

(c) Show that $\mathbf{Z}[\sqrt{-5}]$ is an integral domain that is not a unique factorization domain.

(d) Let t be an indeterminate. Show that $\mathbf{Z}[t]$ is a unique factorization domain that is not a principal ideal domain.

(e) Show that $\mathbf{Z}[(1+\sqrt{-19})/2]$ is a principal ideal domain that is not a euclidean domain. *Hint:* See Dummit & Foote, 3e, pages 277 and 281–282. You may also find helpful discussions on pages 227 (Example (5)) and 229–230.

(f) Give an example of a euclidean domain that is not a field. Justify your assertion.

Solution

We begin by defining the algebraic structures in equation (1) and related terms. We take as given the ring definitions in Chapter 7 of Dummit & Foote, 3e (hereafter, DF3e). We assume all rings are commutative unless noted otherwise. Following the definitions, we present the examples.

Definitions

An **integral domain** is a commutative ring that has a multiplicative identity $1 \neq 0$ and no (nonzero) zero divisors. A **field** is an integral domain in which every nonzero element is a unit.

Let R be an integral domain. A **norm** on R is a map $N : R \to \mathbf{Z}_{\geqslant 0}$ such that $N(0) = 0$. A norm N on R **has a division algorithm** if for all $a, b \in R$ such that $b \neq 0$, there exist $q, r \in R$ such that

$a = qb + r$ with $r = 0$ or $N(r) < N(b)$. We note that q, r need not be unique.[1] A **euclidean domain** is an integral domain on which there exists a norm that has a division algorithm.

An ideal $I \trianglelefteq R$ is **principal** if it is generated by a single element; that is, there exists an $a \in R$ such that $I = (a)$. A **principal ideal domain** is an integral domain for which all ideals are principal.

Let R be an integral domain. An element $r \in R$ is **irreducible** if (i) $r \neq 0$; (ii) $r \notin R^\times$; and (iii) for all $a, b \in R$, if $r = ab$, then $a \in R^\times$ or $b \in R^\times$.[2] Two elements $a, b \in R$ are **associates** if there exists a $u \in R^\times$ such that $a = ub$. (Loosely speaking, a and b differ by a unit.) A **unique factorization domain** is an integral domain R such that for all $r \in R - (\{0\} \cup R^\times)$, the following two conditions are satisfied:

(i) (r has a factorization into irreducibles...) There exist finitely many irreducible elements $p_i \in R$, not necessarily distinct, such that $r = \prod_{i=1}^{n} p_i$.

(ii) (...that is unique up to associates) Given any two such factorizations of r, say $r = \prod_{i=1}^{n_p} p_i$ and $r = \prod_{i=1}^{n_q} q_i$, we have $n_p = n_q$, and we may reorder the factors so that for each i, p_i and q_i are associates.

Example (b): Ring that is not an integral domain

We get examples of rings that are not integral domains by "breaking" at least one part of the definition of an integral domain.

By definition, an integral domain is a commutative ring. Thus, any noncommutative ring is not an integral domain. For example, let R be any nontrivial ring,[3] and consider the ring $M_2(R)$ of 2×2 matrices with entries in R, with addition and multiplication on $M_2(R)$ defined as usual for matrices.[4] By hypothesis, R is nontrivial, so there exist $a, b \in R$ such that $ba \neq 0$. Consider the matrices

$$A = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \qquad \text{and} \qquad B = \begin{pmatrix} 0 & 0 \\ b & 0 \end{pmatrix}$$

We compute

$$AB = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ ba & 0 \end{pmatrix} = BA$$

Thus $M_n(R)$ is not commutative, and therefore not an integral domain. Note that this example is valid even if R is commutative.

[1] For one example, let R be a field. Define $N : R \to \mathbf{Z}_{\geqslant 0}$ by $N(a) = 0$ for all $a \in R$. One readily checks that N satisfies the definition of a norm and has a division algorithm. (In particular, for the division algorithm, one may always take $r = 0$.) Thus a field is a euclidean domain.

For another example, let $R = \mathbf{Z}$. Define $N : \mathbf{Z} \to \mathbf{Z}_{\geqslant 0}$ by $N(a) = |a|$. Then N satisfies the definition of a norm, and one can check (see DF3e, p 271) that it has a division algorithm. Consider $a = 5$ and $b = 3$. The equations $5 = 1 \times 3 + 2$ and $5 = 2 \times 3 - 1$ both satisfy the requirements of the division algorithm, showing that q, r need not be unique.

[2] An element $r \in R$ is **reducible** if it is not irreducible. We won't use this definition here, but it's natural to note. Plus, it's delightfully stereotypical mathematics.

[3] By nontrivial, we mean that the multiplication operation on R does not always output 0. As we have seen, this includes but is not limited to the zero ring.

[4] An argument nearly identical to the one we give will work for the ring $M_n(R)$ of $n \times n$ matrices, for all $n \in \mathbf{Z}_{\geqslant 2}$. Just fill out the matrices A and B with 0.

Let G be any finite group, let R be a commutative ring with multiplicative identity $1 \neq 0$,[5] and let RG be the group ring of G with coefficients in R.[6] It is straightforward to check that the ring RG is commutative if and only if G is commutative. Thus, taking G to be any noncommutative group gives another class of examples of noncommutative rings, and hence rings that are not integral domains.

By definition, an integral domain has a multiplicative identity $1 \neq 0$. Thus, any ring without a multiplicative identity $1 \neq 0$ is not an integral domain. For example, the ring $2\mathbf{Z}$ is not an integral domain. (Note that $2\mathbf{Z}$ satisfies all other axioms of an integral domain.)

By definition, an integral domain has no zero divisors. Thus, any ring with zero divisors is not an integral domain. For example, the ring $\mathbf{Z}/6\mathbf{Z}$ is not an integral domain, because $2, 3 \in \mathbf{Z}/6\mathbf{Z}$ are both nonzero, and $2 \times 3 = 6 \equiv 0$. (Note that $\mathbf{Z}/6\mathbf{Z}$ satisfies all other axioms of an integral domain.)

Example (c): Integral domain that is not a unique factorization domain

See DF3e, pp 229–30 and 286, Example (5).

We consider the ring $\mathbf{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbf{Z}\}$, equipped with addition and multiplication operations analogous to[7] those of $\mathbf{C}$. To see that $\mathbf{Z}[\sqrt{-5}]$ is an integral domain, one can observe that it is a subring of the quadratic field $\mathbf{Q}(\sqrt{-5})$.[8] Fields are integral domains, and subrings of integral domains are integral domains, so $\mathbf{Z}[\sqrt{-5}]$ is an integral domain. Alternatively, one can prove it is an integral domain directly: Let $a, b \in \mathbf{Z}[\sqrt{-5}]$ be arbitrary, say

$$a = a_0 + a_1\sqrt{-5} \qquad\qquad b = b_0 + b_1\sqrt{-5}$$

where $a_0, a_1, b_0, b_1 \in \mathbf{Z}$. Then

$$0 + 0\sqrt{-5} = 0 = ab = (a_0b_0 - 5a_1b_1) + (a_0b_1 + a_1b_0)\sqrt{-5}$$

which is true if and only if the two "coefficients" in the expression on the right are both zero, or equivalently,

$$a_0b_0 = 5a_1b_1 \tag{2}$$
$$a_0b_1 = -a_1b_0 \tag{3}$$

Multiplying equation (2) by b_1 and equation (3) by b_0, we get

$$5a_1b_1^2 = a_0b_0b_1 = -a_1b_0^2$$

in $\mathbf{Z}$. This is equivalent to

$$a_1(5b_1^2 + b_0^2) = 0$$

in $\mathbf{Z}$. Because $\mathbf{Z}$ is an integral domain, the cancellation law implies

$$a_1 = 0 \qquad \text{or} \qquad b_0^2 = -5b_1^2$$

[5] In particular, note that this hypothesis excludes the trivial group.
[6] See DF3e, pp 236–7.
[7] If you prefer, inherited from.
[8] See DF3e, pp 227, 229.

Because all squares in $\mathbf{Z}$ are nonnegative, the second equation is true if and only if $b_0 = 0$ and $b_1 = 0$, that is, if and only if $b = 0$ in $\mathbf{Z}[\sqrt{-5}]$. If the first equation is true — that is, if $a_1 = 0$ — then equations (2) and (3) reduce to

$$a_0 b_0 = 0 \qquad \text{and} \qquad a_0 b_1 = 0$$

If $a_0 = 0$, then $a = 0$ in $\mathbf{Z}[\sqrt{-5}]$, and we are done. If $a_0 \neq 0$, then again using the fact that $\mathbf{Z}$ is an integral domain, we must have $b_0 = 0$ in the first equation and $b_1 = 0$ in the second equation, so that $b = 0$ in $\mathbf{Z}[\sqrt{-5}]$.

To see that $\mathbf{Z}[\sqrt{-5}]$ is not a UFD, consider two factorizations of the element 6:

$$(1 + \sqrt{-5}) \times (1 - \sqrt{-5}) = 6 = 2 \times 3$$

If we can show that the factors $1 \pm \sqrt{-5}, 2, 3$ are irreducible, then we are done. To do this, we can use the field norm

$$\begin{aligned} N : \mathbf{Q}(\sqrt{-5}) &\to \mathbf{Q} \\ a + b\sqrt{-5} &\mapsto a^2 + 5b^2 \end{aligned}$$

restricted to $\mathbf{Z}[\sqrt{-5}]$ (note that the codomain of the restricted norm is $\mathbf{Z}$).[9] We compute the norms

$$N(1 \pm \sqrt{-5}) = 6 \qquad N(2) = 4 \qquad N(3) = 9$$

One can check that N is multiplicative. So if an element factors in $\mathbf{Z}[\sqrt{-5}]$, then the norm of each factor is an integer that divides that element's norm. For example, if there exist $\alpha, \beta \in \mathbf{Z}[\sqrt{-5}]$ such that $1 + \sqrt{-5} = \alpha\beta$, then

$$6 = N(1 + \sqrt{-5}) = N(\alpha\beta) = N(\alpha)N(\beta)$$

as an equation in $\mathbf{Z}$. A case analysis[10] of the possible values of the factors' norms shows that the only factorizations of $1 \pm \sqrt{-5}$, 2, and 3 involve units, so they are irreducible.

Example (d): Unique factorization domain that is not a principal ideal domain

See DF3e, pp 252, Example (3); 273, Example (1); 279, Example (1); and 304–5, Theorem 7.

Consider $\mathbf{Z}[t]$. We will show below that $\mathbf{Z}$ is a euclidean domain. Hence, by the implications in equation (1), $\mathbf{Z}$ is a unique factorization domain.[11] Hence $\mathbf{Z}[t]$ is a unique factorization domain, by Theorem 9.7.

We claim that the ideal $(2, t)$ is not principal. Because $\mathbf{Z}[t]$ is a commutative ring, the ideal

$$(2, t) = \{2p(t) + tq(t) \mid p(t), q(t) \in \mathbf{Z}[t]\}$$

Observe that $f(t) \in (2, t)$ if and only if $2 \mid f(0)$. In particular, $1 \notin (2, t)$, so $(2, t)$ is a proper ideal. Suppose for the sake of contradiction[12] that $(2, t)$ were principal. Then by definition, there exists an $a \in \mathbf{Z}[t]$ such that $(2, t) = (a)$. Because $2 \in (2, t) = (a)$, there exist $b \in \mathbf{Z}[t]$ such that $2 = ab$. The degree function on $\mathbf{Z}[t]$, which maps nonzero polynomials to their degree and the zero polynomial to $-\infty$, satisfies two important conditions:

[9] See DF3e, pp 229–30.

[10] See DF3e, p 273.

[11] See also DF3e, p 287, Theorem 14.

[12] We follow the argument in DF3e, p 252, Example (3).

1. For all $f \in \mathbf{Z}[t] - \{0\}$, $\deg f \in \mathbf{Z}_{\geqslant 0}$.

2. Because $\mathbf{Z}$ is an integral domain,[13] for all $f, g, h \in \mathbf{Z}[t]$ such that $f = gh$,

$$\deg f = \deg g + \deg h$$

Applying these conditions to the equation $2 = ab$, we get

$$0 = \deg 2 = \deg a + \deg b$$

so both polynomials a and b must be constants. We may view the equation $2 = ab$ in $\mathbf{Z}$ and conclude that either (i) $a = \pm 1$ and $b = \pm 2$, or (ii) $a = \pm 2$ and $b = \pm 1$. In case (i), $(a) = (1)$, contradicting the fact that $(a) = (2, t)$ is a proper ideal. In case (ii), $t \in (2, t) = (a) = (2)$ implies that there exists a $b \in \mathbf{Z}[t]$ such that $t = 2b(t)$. All coefficients of the polynomial $2b(t)$ are divisible by 2, whereas the coefficient of t is not, so equality of the two is a contradiction. We conclude that $(2, t) \trianglelefteq \mathbf{Z}[t]$ is not principal, and therefore $\mathbf{Z}[t]$ is not a principal ideal domain.

Example (e): Principal ideal domain that is not a euclidean domain

See DF3e, pp 229-30, 276–7, 282.

Consider $\mathbf{Z}[(1 + \sqrt{-19})/2] = \{a + b(1 + \sqrt{-19})/2 \mid a, b \in \mathbf{Z}\}$. We can show that this ring is a principal ideal domain but not a euclidean domain as follows:

1. Define norm, positive norm, and Dedekind–Hasse norm.[14]

2. Cite Proposition 8.9 (DF3e, p 281): Let R be an integral domain. Then R is a principal ideal domain if and only if there exists a Dedekind–Hasse norm on R.

3. Show that the function

$$\begin{aligned} N : \mathbf{Z}[(1 + \sqrt{-19}/2)] &\to \mathbf{Z} \\ a + b(1 + \sqrt{-19})/2 &\mapsto a^2 + ab + 5b^2 \end{aligned}$$

   is a Dedekind–Hasse norm on $\mathbf{Z}[(1 + \sqrt{-19})/2]$.[15] Thus the ring is a principal ideal domain.

4. Define universal side divisors.[16]

5. Cite Proposition 8.5 (DF3e, p 277): Let R be an integral domain that is not a field. If R is a euclidean domain, then R has universal side divisors.

6. Show that $\mathbf{Z}[(1 + \sqrt{-19})/2]$ has no universal side divisors.[17]

[13] Why is this condition important?

[14] See DF3e, p 281

[15] See DF3e, p 282, Example.

[16] See DF3e, p 277. The second definition more closely resembles notions we may be used to from the euclidean algorithm

[17] See DF3e, p 277, Example.

Example (f): Euclidean domain that is not a field

Consider the ring of integers, $\mathbf{Z}$. Define $N : \mathbf{Z} \to \mathbf{Z}_{\geqslant 0}$ by $N(a) = |a|$. One can check that N satisfies the definition of a norm, and that it has a division algorithm.[18] Thus $\mathbf{Z}$ is a euclidean domain. However, $\mathbf{Z}^\times = \{\pm 1\} \neq \mathbf{Z} - \{0\}$ — for example, $2 \in \mathbf{Z}$ has no multiplicative inverse — so $\mathbf{Z}$ is not a field.

As another example, let F be a field, and consider the ring $F[t]$ of polynomials in one indeterminate t with coefficients in F.[19] Define

$$\begin{aligned} N : F[t] &\to \mathbf{Z}_{\geqslant 0} \\ f &\mapsto \begin{cases} \deg f & \text{if } f \neq 0 \\ 0 & \text{if } f = 0 \end{cases} \end{aligned}$$

One can check that N satisfies the definition of a norm, and that it has a division algorithm.[20] Thus $F[t]$ is a euclidean domain. However, $F[t]^\times = F^\times \neq F[t] - \{0\}$ — for example, $t \in F[t]$ has no multiplicative inverse — so $F[t]$ is not a field.

[18] See DF3e, p 271, Example (1).
[19] See DF3e, pp 234–5.
[20] See DF3e, p 271, Example (2).